HEALTH AFFAIRS

TRICARE
Management
Activity

Privacy Specific Topics

HIPAA Training

TMA Privacy Office

Privacy Specific Topics

Agenda

- Personal Representatives
- Allowances for Family Members
- Provider/Patient Communication
- Public Directories and the Clergy
- Media
- Business Associates
- Other Agreements to Protect Data
- Research and Marketing Under HIPAA
- DoD/DVA Sharing

Privacy Specific Topics

Training Objectives

- Upon completion of this course, you will be able to:
  - Identify personal representatives
  - Describe allowances for family members
  - Identify appropriate provider patient communication
  - Explain public directories and clergy requirements
  - Describe how to share PHI with the media
  - Describe Business Associates
  - Explain other agreements to protect data
  - Explain research and marketing under HIPAA
  - Identify allowable sharing between DoD and DVA

Personal Representatives

Objectives

- Upon completion of this lesson, you will be able to:
  - Determine when someone is or is not a personal representative
  - Identify what a personal representative can do
  - Explain the limitations and state laws
  - Describe the exceptions

Personal Representatives

- The HIPAA Privacy Rule allows providers, health plans and clearinghouses to treat an individual's personal representative (PR) as if they were the individual
- Categories:
  - Adult or emancipated minor
  - Unemancipated minor
  - Deceased individuals
  - Abuse, neglect, and endangerment situations

Personal Representatives

Adult or Emancipated Minor

- PR is a person with legal authority to make health care decisions on behalf of individual
- Examples:
  - Health care power of attorney
  - Court appointed legal guardian
  - General power of attorney

Personal Representatives
Unemancipated Minor

- PR is a parent, guardian, or other person acting *in loco parentis* with legal authority to make health care decisions on behalf of the minor child
- Examples:
  - Parent
  - Court appointed guardian
  - Healthcare or general power of attorney

Personal Representatives

Deceased Individual

- PR is a person with legal authority to act on behalf of the decedent to the estate (not restricted to health care decisions)
- Examples:
  - Executor of the estate (Will)
  - Administrator (No Will)

Personal Representatives

What the PR Can Do

- The Personal Representative may:
  - Be provided with information about the individual's care and condition
  - Use PHI to make health care decisions
  - Authorize disclosures of PHI
  - Exercise the individual's rights, e.g. ask for accounting of disclosures

Personal Representatives
Limitations and State Laws

- If authority to act is limited, then rights with respect to PHI is limited
  - e.g., if power of attorney is limited to use of artificial life support, then PR can access PHI related to that health care decision
- Rule defers to state law with regard to rights of parents/guardians of minors

Personal Representatives

Exceptions (1 of 2)

- Do not treat the PR as the individual when:
  - An MTF has a reasonable belief that the individual may be subject to domestic violence, abuse or neglect by the PR
  - Treating the PR as the individual could in some way endanger the individual
  - An MTF believes, in its professional judgment, that it is not in the best interest of the individual to treat the PR as the individual

Personal Representatives

Exceptions (2 of 2)

- A parent is not the PR when:
  - State or other law does not require the consent of a parent before a minor can obtain a particular service, and the minor consents to the service
  - A court determines or other law authorizes someone other than the parent to make decisions for a minor
  - A parent agrees to a confidential relationship between the minor and the physician

Personal Representatives

Deceased Individuals

- Rights and protections granted under HIPAA continue to apply to the PHI of deceased individuals
- You must continue to protect the confidentiality of the PHI
- Deceased persons PR may now exercise control over use and disclosure of PHI (right of access, authorizations for disclosure etc.)
- You may disclose PHI without an authorization to:
  - Coroners and medical examiners
  - Funeral directors
  - Organizations aiding in the transplantation of organs, eyes and tissue

Personal Representatives

Summary

- You should now be able to:
  - Determine when someone is or is not a personal representative
  - Identify what a personal representative can do
  - Explain the limitations and state laws
  - Describe the exceptions

Allowances for Family Members

Allowances for Family Members
Objectives

- Upon completion of this lesson, you will be able to:
  - Identify when sharing is allowed with family members
  - Describe examples of permitted disclosures

Allowances for Family Members

Sharing with Family Members

- Sharing is allowed with family members if:
  - An individual does not object, an MTF may disclose limited information to family members or others regarding the individual’s care when:
    - An individual is present and agrees or does not object when given the opportunity
    - An individual is not present, the provider may use their professional judgment as to the best interest of the individual

Allowances for Family Members

Permitted Disclosures

- Examples of Permitted Disclosures:
  - When a patient's mobility is limited and a family member is driving them home from the hospital
  - When a patient is accompanied by a family member to a medical appointment, and it is clear that the person will be involved in the patient's care
  - Doctor may provide information to family members who have brought the patient to the emergency room
  - A hospital may discuss a patient's payment options with an adult, child, or spouse
  - Pharmacy may allow a family member to pick up an individual's prescription or medical supplies

Summary

- You should now be able to:
  - Identify when sharing is allowed with family members
  - Describe examples of permitted disclosures

Other Communication Within HIPAA

Other Communication within HIPAA

Objectives

- Upon completion of this lesson, you will be able to:
  - Identify appropriate Provider-Patient Communication
  - Identify use and restrictions of public directories and the clergy
  - Identify information that can be shared with the media

Other Communication within HIPAA

Permissible Communications

- Reference from the Rule
- Provider-Patient Communication
- Public Directories and the Clergy
- Media

Other Communication within HIPAA

Provider-Patient Communication

- Providers may remind patients of appointments, test result availability, and prescriptions through:
  - Answering machines
  - Mailings
  - Messages with family members or others answering the phone
- The minimum necessary rule applies

Other Communication within HIPAA

Public Directories and the Clergy

- Health Care facilities may maintain directories of current patients with the following information:
  - Name
  - Location in facility
  - Condition in general terms
  - Religious affiliation
- Except for religious affiliation, the information may be disclosed to anyone who asks for the individual by name
  - Religious affiliation may be disclosed only to member of the clergy

Other Communication within HIPAA

Public Directories- Condition

- Only one-word condition description should be made
  - Undetermined: Patient awaiting physician and assessment or when unknown
  - Good: Vital signs are stable and within normal limits Patient is conscious and indicators are excellent
  - Fair: Vital signs are stable and within normal limits Indicators are favorable
  - Serious: Vital signs may be unstable and not within normal limits Patient is acutely ill and indicators are questionable
  - Critical: Vital signs are unstable and not within normal limits Patient may be unconscious and indicators are unfavorable

Other Communication within HIPAA

Public Directories- Location

- The patient's location (room number) may be included in the patient directory to facilitate visits by family and friends and deliveries of cards and flowers, etc
  - However, as part of your policy, the patient's location should not be given out to the media
  - Keep in mind, a patient can elect not to be included in the patient directory and that request should be honored
  - Caution should be exercised to ensure that the location given is not generally known or associated with a particular specialty of care that could confirm a diagnosis

Other Communication within HIPAA

Public Directories- Restrictions

- Patient must have prior opportunity to agree or object to being included on the public directory
  - Oral agreement or objection is allowed
- In an emergency situation or if a patient is unable to agree or object, use professional judgment
  - Provide opportunity to agree or object as soon as possible

Media

- HIPAA does not expressly prohibit disclosure of patient information to the media
  - TMA requires that hospitals must adopt policies that prohibit disclosure of information other than patient condition and location to the media without patient authorization
- If the media does get involved, the patient must sign an authorization form
- CE should have a central release authority (single site) for media, VIP, etc

Other Communication within HIPAA

Media- Activities

- Activities that involve the media could include:
  - Drafting of a detailed statement by the hospital (which goes beyond the one-word condition) that is approved by the patient or their legal representative
  - Taking photographs of patients
  - Interviewing patients
- Next of kin or guardians must sign when a person is unable to do so in their own right (incapacitated, minors)

Other Communication within HIPAA

Media- Patient Access

- Media should not contact patients directly. If media does get involved, appropriate hospital staff should be present at all times
- Hospitals should consider denying access if it’s determined that a patient’s medical condition could be aggravated or that patient care could be interfered with
- A hospital representative should accompany media at all times and should deny access to certain areas of the hospital (such as operating rooms, maternity, pediatrics, emergency rooms, etc.)
- Check with local command policy for more guidance

Other Communication within HIPAA

Media- Public Record

- “Public Record” cases are those cases where certain situations are reportable to public authorities (such as Department of Health and Human Services (DHHS)), law enforcement or public health authorities
- “Public Record” cases are no different than other patients, so a hospital should handle their privacy rights in the same way all patients are dealt with – even under HIPAA
- Celebrities and public officials are no different than any other patient and should be treated as such

Other Communication within HIPAA

Summary

- You should now be able to:
  - Identify appropriate Provider-Patient Communication
  - Identify use and restrictions of public directories and the clergy
  - Identify information that can be shared with the media

Business Associates

Business Associates
Objectives

- Upon completion of this lesson, you will be able to:
  - Define business associates
  - Describe business associate functions
  - Identify business associates
  - Describe safeguard requirements for business associates
  - Explain business associate agreements
  - Identify business associate training requirement
  - Explain protections for whistleblowers & crime victims

Who is a Business Associate?

- “A person or entity who provides certain functions, activities, or services for or to a covered entity, involving the use and/or disclosure of protected health information”
  - Can be a health care provider, health plan, or another covered entity
  - Cannot be a member of the health care provider, health plan, or other covered entity's workforce
  - Excludes covered entities who disclose protected health information to providers for treatment purposes

Business Associates
Basic Conditions

- Three basic conditions define a business associate, including:
  - Performs, or helps perform, work that uses or discloses individually identifiable health information on behalf of the covered entity
  - Work being performed is a “covered function” (activities that pay for, or provide health care) regulated by the rule
  - Person performing work does not belong to the covered entity’s workforce

Business Associate Functions

- Functions or activities that involve the use or disclosure of PHI, include:
  - Legal
  - Actuarial
  - Accounting
  - Billing
  - Consulting
  - Data Aggregation
  - Claims Processing
  - Utilization Review
  - Quality Assurance
  - Management
  - Administrative
  - Accreditation
  - Financial Services

Identifying a Business Associate (1 of 2)

- Inventory existing contracts
- Identify other business associates by performing a data flow analysis of PHI
- Look at the functions performed by the third parties, not just their predominant role
  - For example, a provider may have a payer as a business associate if it provides assistance for the provider's 'wellness programs'
  - Clearinghouses may be business associates if they perform translation services
  - Medical supply houses may serve as conduits to move PHI back to manufacturers

Identifying a Business Associate (2 of 2)

- Consider organizations that perform the following services:
  - Legal and actuarial
  - Accreditation and consulting
  - Software and hardware vendors
  - Outsourcing & contract services
  - Temp agencies
  - Medical transcription services
  - Financial management

Business Associates
Safeguards

- HIPAA Privacy/Security Rules extend safeguards for PHI to persons or entities who work with PHI on a CE’s behalf
  - The BA must comply with the requirements of the Privacy/Security Rules
- HIPAA requires including the requirement to comply with the safeguards as part of the contracts governing performance of the work (i.e., “business associate agreements”)

Business Associate Agreements (BAA)

- Privacy BAAs were required to be in place by April 14, 2003; Security BAAs were required by April 20, 2005
- The rule requires covered entities to establish agreements between themselves and entities with whom PHI is shared
- The rule does not require covered entities to monitor, audit or oversee business associates for HIPAA compliance. They are expected to periodically verify that the business associates are complying with the agreements

Business Associates

BAA- Content (1 of 2)

- Use and disclose PHI only for purposes permitted by the contract or HIPAA
- Use appropriate safeguards to prevent use or disclosure of the PHI other than as permitted by the contract
- Report to the covered entity any use or disclosure of the information not provided for by its contract
- Ensure that any agents, including a subcontractor, to whom it provides PHI agrees to the same restrictions and conditions that apply to the business associate with respect to the PHI

BAA- Content (2 of 2)

- Provide PHI for amendment and incorporate any amendments to PHI
- Make available the information required to provide an accounting of disclosures
- Provide internal practices, books, and records relating to the use and disclosure of PHI to the Secretary of HHS for purposes of determining the covered entity's compliance with HIPAA
- Return or destroy all PHI received from, or created or received by the business associate on behalf of, the covered entity upon termination of the contract

Business Associate Training

- All Business Associates must complete HIPAA Privacy training if:
  - The business associates' workspace is within the physical confines of the MTF, the TMA provided web based training tool may be used to train the BA
  - The business associates' workspace is not within the physical confines of the MTF, the BA is responsible for providing its own training

Business Associates

Whistleblowers and Crime Victims

- Workforce members or business associates may disclose PHI to the proper authorities or their attorney if they believe the CE is:
  - Engaged in unlawful activity
  - Violating professional or clinical standards
  - Potentially endangering patients, workers or the public through care services or conditions
- Workforce members who are victims of a crime may disclose to law enforcement officers those elements of the suspect's PHI that identify the suspect

Summary

- You should now be able to:
  - Define business associates
  - Describe business associate functions
  - Identify business associates
  - Describe safeguard requirements for business associates
  - Explain business associate agreements
  - Identify business associate training requirement
  - Explain protections for whistleblowers & crime victims

Other Agreements to Protect Data

Other Agreements to Protect Data

Objectives

- Upon completion of this lesson, you will be able to:
  - Define Data Use Agreements (DUA)
  - Explain Requirements for DUAs
  - Define Memorandum of Agreements (MOA)
  - Explain Requirements for MOAs
  - Clarify Relationship to Business Associate Agreements

Other Agreements to Protect Data

What are Data Use Agreements (DUA)

- Data Use Agreements (DUAs) are an integral part of the data use approval process
- DUAs are established between a DoD and a non-DoD entity, including contractors, researchers, etc
- The agreements:
  - Delineate the confidentiality of the Privacy Act and DoD's data use policies and procedures
  - Inform data users of these requirements and are a means of obtaining their agreement to abide by these requirements
  - Are a control mechanism through which DoD can track the location of its data and the reason for the release of the data

Other Agreements to Protect Data

DUA Requirements

- DoD has developed a number of standard Data Use Agreements, all of which are designed to ensure that:
  - Requesters use DoD data only for the purpose(s) cited in the request
  - Requesters will not release DoD data to other organizations without prior written DoD approval
  - Requesters will take reasonable steps to implement appropriate procedural, administrative, technical, and physical safeguards to prevent unauthorized use
  - Requesters do not publish any information that identifies individual beneficiaries or providers, or permits the identity of a beneficiary or provider to be deduced
  - A limit is established on the period of time a requester may retain DoD data before the data must be destroyed

Other Agreements to Protect Data

What are Memorandums of Agreement

- Memorandums of Agreement (MOAs) are an integral part of the data process
- MOAs are established between government agency's to allow for sharing of MHS data
- The agreements:
  - Delineate the confidentiality of the Privacy Act and DoD's data use policies and procedures
  - Inform data users of these requirements and serve as a means of obtaining their agreement to abide by these requirements
  - Are a control mechanism through which DoD can track the location of its data and the reason for the release of the data

Other Agreements to Protect Data

MOA Requirements

- MOA are designed to ensure that requesters:
  - Use MHS data only for the purpose(s) cited in the request
  - Will meet TMA security and privacy standards when re-releasing data to a third party
  - Notify the CE of all third parties with whom data is shared and provide the CE with a copy of the sharing agreement
  - Will take reasonable steps to implement appropriate procedural, administrative, technical, and physical safeguards to prevent unauthorized use
  - Do not publish any information that identifies individual beneficiaries or providers, or permits the identity of a beneficiary or provider to be deduced
  - Have their MOA reviewed annually for applicability and appropriateness

Other Agreements to Protect Data

Relationship to BA Agreements

- Both DUAs and MOAs include business associate agreement language
- Those organizations which hold a DUA or MOA are subject to the rules of business associates as put forth in HIPAA

Other Agreements to Protect Data

Summary

- You should now be able to:
  - Define Data Use Agreements (DUA)
  - Explain Requirements for DUAs
  - Define Memorandum of Agreements (MOA)
  - Explain Requirements for MOAs
  - Clarify Relationship to Business Associate Agreements

Research and Marketing Under HIPAA

Objectives

- Upon completion of this lesson, you will be able to:
  - Define research and marketing under HIPAA
  - Identify the exceptions for research and marketing
  - Describe how research is explained in the NOPP
  - Explain the applicability of other rules in regards to research
  - Identify the appropriate authorization required for research
  - Explain the transition provision for research
  - Describe the marketing rule

What is Research?

- Any systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalized knowledge
- Research does not include:
  - Quality assessment and improvement activities, such as outcomes evaluation or development of clinical guidelines
  - Activities for generalized knowledge for population health

General Rule and Exceptions

- Research-related uses and disclosures of PHI require prior written authorization except when:
  - The PHI will not leave the covered entity, will be used solely for reviews in preparation for research, and the researcher represents to the covered entity that such access is essential
  - The PHI refers solely to deceased persons and the researcher again asserts to the covered entity that access is necessary for the research purpose
  - An Institutional Review Board (IRB) or a Privacy Board determines that a waiver of the authorization requirement is appropriate

Research in Relation to Notice of Privacy Practices (NoPP)

- The MHS NoPP informs patients and beneficiaries that:
  - The MHS "may disclose your protected health information to researchers when authorized by law, for example, if their research has been approved by an institutional review board that has reviewed the research proposal and established protocols to ensure the privacy of your protected health information"

Research and Marketing Under HIPAA

Applicability of Other Rules

- The HIPAA rules regarding research do NOT replace other applicable laws such as the Common Rule and the FDA human subject protection rules
  - All requirements for informed consent and IRB review from these other regulations must be met
- The HIPAA rules regarding the use and disclosure of minimum necessary information apply to information used and disclosed for research

Research- Disclosure Accounting

- Information disclosed for research is subject to the HIPAA disclosure accounting requirement
- For studies involving more than 50 records, the requirement may be met by providing individuals with:
  - A list of all protocols for which their PHI may have been disclosed pursuant to a waiver/exception
  - The purpose of those studies and the types of PHI sought
  - The timeframes of those disclosures
  - A researcher’s name and contact information for each study

Research- Data Access

- The individual’s right to access their PHI may be suspended while the clinical trial is in progress if the individual agreed to the denial of access when consenting to participate
  - The individual must be informed that the right to access will be reinstated at the conclusion of the study
- Covered entities do not need an authorization or waiver from an IRB or Privacy board to release information for research if the information has been either de-identified or is part of a limited data set and the researcher has a data use agreement

HIPAA Research Authorization (1 of 3)

- Research authorizations must meet all of the applicable HIPAA requirements for authorizations except that they do not require an expiration date
- Authorizations must be in writing, signed, and contain the following elements:
  - A description of the information to be used or disclosed in a specific or meaningful fashion
  - The name or specific identification of the person(s) or class of persons authorized to make the requested use or disclosure
  - The name or specific identification of the person(s) or class of persons to whom the CE may make the disclosure

HIPAA Research Authorization (2 of 3)

- Authorizations must be in writing, signed, and contain the following elements (cont.):
  - A description of each purpose of the requested use or disclosure (may be at the request of the individual when the individual initiates the authorization)
  - An expiration date or expiration event, except it may say “none” or “end of the research study” for research authorizations
  - Signature of the individual and date (and a description of the representative’s authority to act for the individual if signed by a personal representative)
  - A statement of the individual’s right to revoke the authorization and a description of how they may do so

HIPAA Research Authorization (3 of 3)

- Authorizations must be in writing, signed, and contain the following elements (cont.):
  - The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization. (While the CE may not normally condition treatment on obtaining an authorization they may condition “research related treatment”)
  - The potential for information disclosed pursuant to the authorization to be subject to re-disclosure by the recipient and no longer protected by HIPAA

Research and Marketing Under HIPAA

Transition Provisions

- PHI created or received prior to the compliance date may still be used or disclosed for specific studies if one of the following was obtained prior to the compliance date, April 14, 2003:
  - An authorization from the individual
  - The informed consent of the individual to participate in the study
  - A waiver by an IRB in accordance with the Common Rule or FDA's human subject protection regulations

What is Marketing?

- "To make a communication about a product or service to encourage recipients of the communication to purchase or use the product or service"
- Marketing is:
  - Disclosing patient lists to third parties for independent marketing
  - Selling patient lists
- Marketing is <u>not</u>:
  - Communications related to care coordination
  - Alternative treatment recommendations
  - Describing participating providers or the plan
  - Describing services offered
- Marketing activities require authorizations

Research and Marketing Under HIPAA

Marketing Exclusions

- HIPAA excludes the following from the definition of marketing:
  - Information provided for the purpose of furthering or managing the treatment of an individual (ex. Information or recommendations about various treatment options, information about a smoking cessation program)
  - Information about coverage or payment (ex. Existing benefits as well as other products or services optionally available to a health plan enrollee)
  - Population-oriented communications that promote health in “a general manner” provided they do not endorse a specific product or service

Marketing Rule

- All marketing efforts that do not meet one of the exceptions or exclusions specified in the rule require a prior written authorization
- Authorization must contain all of the HIPAA required fields and information
  - Approved authorization form is available on the TMA Privacy Office website
  - The correct form is the DD Form 2870
  - Retain according to local policies and procedures

Summary

- You should now be able to:
  - Define research and marketing under HIPAA
  - Identify the exceptions for research and marketing
  - Describe how research is explained in the NOPP
  - Explain the applicability of other rules in regards to research
  - Identify the appropriate authorization required for research
  - Explain the transition provision for research
  - Describe the marketing rule

Department of Defense/Department of Veteran’s Affairs Sharing

DoD/DVA Sharing

Objectives

- Upon completion of this lesson, you will be able to:
  - Identify when PHI can be given to the Veteran's Health Administration (VHA) for treatment
  - Define when PHI can be provided for determining benefits prior to separation
  - Explain requirement for Veteran's Support/Service Organizations to receive PHI
  - Clarify the required by law provision

DoD/DVA Sharing

When Can PHI be Provided to VHA?

- HIPAA Privacy Rule states that “a covered entity may disclose protected health information for treatment activities of a health care provider”
  - Sharing of PHI between DoD and VHA for the purpose of treatment can be accomplished at the point where a decision is made to seek care for an individual in the VHA
- HIPAA Privacy Rule defines treatment as “the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another”

DoD/DVA Sharing

Disclosure of PHI for Determining Benefits

- PHI may be disclosed to DVA when an individual who is a member of the armed forces upon separation or discharge of the individual from military service for the purposes of the determination by DVA of the individuals eligibility for or entitlement to benefits
- DVA may use and disclose protected health information to components of the Department that determine eligibility for or entitlement to, or that provide, benefits
- PHI can be shared when an individual signs a valid HIPAA-compliant authorization granting permission to a covered entity to share their data with another specified covered entity

DoD/DVA Sharing

Veteran's Support/Service Organizations Receiving PHI

- DoD requires a HIPAA compliant authorization form to be initiated by the individual service member prior to information being provided to non-government groups
- Veterans Support/Service organizations often request PHI of hospitalized service members to help these individuals identify and apply for DVA benefits they are entitled to receive
  - Disabled American Veterans (DAV)
  - Veterans of Foreign Wars (VFW)
- These groups have no direct right to receive PHI

DoD/DVA Sharing

Required By Law Provision

- "A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law"
- A TMA determination would need to be made to determine whether the sharing in question falls within the scope of the provided authority

Summary

- You should now be able to:
  - Identify when PHI can be given to the Veteran's Health Administration (VHA) for treatment
  - Define when PHI can be provided for determining benefits prior to separation
  - Explain requirement for Veteran's Support/Service Organizations to receive PHI
  - Clarify the required by law provision

Presentation Summary

- You should now be able to:
  - Identify personal representatives
  - Describe allowances for family members
  - Identify appropriate provider patient communication
  - Explain public directories and clergy requirements
  - Describe how to share PHI with the media
  - Describe business associates
  - Explain other agreements to protect data
  - Explain research and marketing under HIPAA
  - Identify allowable sharing between DoD and DVA

Resources

- DoD 6025.18-R, “DoD Health Information Privacy Regulation”, January 2003
- www.tricare.osd.mil/tmaprivacy/HIPAA.cfm
- privacymail@tma.osd.mil for subject matter questions
- hipaasupport@tma.osd.mil for tool related questions
- http://www.tricare.osd.mil/tmaprivacy/Mailing-List.cfm to subscribe to the TMA Privacy Office E-News
- Service HIPAA Privacy representatives

HEALTH AFFAIRS

TRICARE
Management
Activity

Please fill out your critique

Thanks!